

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

6/7/2010

SUBJECT:

Multiple Adobe Products are Prone to a Remote Code Execution Vulnerability

OVERVIEW:

A vulnerability has been discovered in the Adobe Acrobat, Adobe Reader and Adobe Flash Player applications that could allow attackers to execute arbitrary code on affected systems. Adobe Reader allows users to view Portable Document Format (PDF) files. Adobe Acrobat offers users additional features such as the ability to create PDF files. Adobe Flash Player is a multimedia and application player used to enhance the user experience when visiting web pages or other media which incorporate Flash (.swf) files.

Exploitation can occur if a user visits or is redirected to a malicious webpage or if a user opens a malicious file designed to take advantage of this vulnerability, including opening a malicious attachment. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

Adobe has indicated that this vulnerability is actively being exploited and there is no patch available at this time. Adobe has, however, provided mitigation advice. Please see the Recommendations section below.

SYSTEMS AFFECTED:

Adobe Flash Player 10.0.45.2, 9.0.262, and earlier 10.0.x and 9.0.x versions.
Adobe Reader and Acrobat 9.3.2 and earlier 9.x versions.

RISK:**Government:**

Large and medium government entities: **High**
Small government entities: **High**

Businesses:

Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:

A memory error corruption vulnerability has been identified in multiple Adobe products that could allow for remote code execution when opening maliciously crafted Flash content. The memory error corruption vulnerability is triggered by opening a specially crafted Flash (.swf) file or by opening a .pdf file with embedded malicious Flash content. Adobe Reader 9.x and Adobe Acrobat 9.x products are vulnerable via the 'authplay.dll' which allows those products to view Flash content within PDF files. Successful exploitation may result in an attacker gaining the same privileges as the logged on user. Depending on

the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with user level of logged on user. Failed exploitation could result in denial-of-service conditions.

Adobe has indicated that this vulnerability is being actively exploited over the internet.

Adobe is reporting that Flash player 10.1.53.64 RC7, released on June 2, 2010, does not appear to be vulnerable.

Note that Adobe Flash player 10.1.x versions have all been BETA releases.

Adobe Reader 8.x and Adobe Acrobat 8.x products are not vulnerable.

Adobe has not released a patch for this vulnerability at this time, and is currently recommending users delete, rename or remove access to the 'authplay.dll' that ships with Adobe Reader and Adobe Acrobat 9.x products to mitigate the threat for those products.

To disable Flash support in *Adobe Reader 9* on Microsoft Windows, delete or rename these files:

"%ProgramFiles%\Adobe\Reader 9.0\Reader\authplay.dll"

To disable Flash support in *Adobe Acrobat 9* on Microsoft Windows, delete or rename these files:

"%ProgramFiles%\Adobe\Acrobat 9.0\Acrobat\authplay.dll"

The above mitigation steps will result in reduced functionality within Adobe Acrobat and Adobe Reader applications. The file locations listed above may vary due to customized installations.

Antivirus Vendors have released signatures that will protect against the currently released exploit.

RECOMMENDATIONS:

The following actions should be taken:

- Install the appropriate Adobe patch as soon as it becomes available after appropriate testing.
- Consider disabling Flash support in Adobe Acrobat and Adobe Reader by the steps noted above.
- Rename or remove access to the 'authplay.dll' that ships with Adobe Reader and Adobe Acrobat.
- Ensure that all antivirus software is up to date with the latest signatures.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.
- If you believe you have been affected by attacks exploiting this vulnerability, please follow your organization's policies for incident reporting.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/advisories/apsa10-01.html>
<http://blogs.adobe.com/psirt/>

Secunia:

<http://secunia.com/advisories/40026>
<http://secunia.com/advisories/40034>

Security Focus:

<http://www.securityfocus.com/bid/40586>

VUPEN:

<http://www.vupen.com/english/advisories/2010/1348>

<http://www.vupen.com/english/advisories/2010/1349>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1297>